

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Advanced Methods to Target and Eliminate)	CG Docket No. 17-59
Unlawful Robocalls)	
)	
Call Authentication Trust Anchor)	WC Docket No. 17-97

WRITTEN EX PARTE

5th/4th FURTHER NOTICES OF PROPOSED RULEMAKING
Re: Gateway Providers & Foreign-Originated Calls

ZipDX submits these comments as a result of recent events, including:

- Vermont Attorney General robocalling complaint against provider TCA VOIP¹
- USTelecom, et al March 28 2022 ex parte meeting in these dockets²

ZipDX has highlighted on numerous occasions that there are a handful of providers that are responsible for facilitating an enormous number of illegal robocalls. The Vermont Complaint is illustrative.

Per the Complaint Appendix, TCA VOIP was getting tracebacks as far back as August of 2020 (19 months ago) related to fraud calls coming from My Country Mobile. This flow of calls continued unabated, per the listing of tracebacks in the Appendix.

The Complaint indicates (at p. 91) that the AG, joined by the Social Security Office of Inspector General, met with TCA VOIP on August 19, 2021 (7 months ago). During this meeting, the Complaint says (at p, 102) “TCA VOIP indicated that it would work to address illegal robocalls from its upstream providers....”

At p. 103, the Complaint says “Despite the assurances of TCA VOIP, the problems with TCA VOIP facilitating unlawful traffic continued. CDRs from TCA VOIP on August 30, 2021, demonstrate that it completed 4,619,062 calls that day, including 3,015,165 calls from My Country Mobile, its principal customer throughout this investigation.” At p. 105, the Complaint states “The CDRs for these 3,015,165 calls revealed that many were illegal robocalls” and gives supporting evidence. At p. 106, we see “The Vermont Office of Attorney General informed TCA VOIP of these findings of continued illegal traffic by email on September 9, 2021, at 7:06 p.m.” P. 107 says “Rather than concede the obvious-that TCA VOIP had determined to continue to host fraudulent traffic-TCA VOIP responded: ‘The traffic is 99.999% legitimate with 1 out of

¹ <https://ago.vermont.gov/blog/2022/03/18/ag-donovan-sues-illegal-robocall-carrier-tca-voip/>

² <https://www.fcc.gov/ecfs/file/download/DOC-5ff75a4a61000000-A.pdf>

100 million fraudulent calls.’ TCA VOIP denied it was ‘willfully blind as to the illegal character of that traffic,’ adding, ‘It is not the balance I want but it's the business we reach.’”

At p. 113, the Complaint says “And TCA VOIP continued to facilitate illegal robocalls and continued to show up in ITG tracebacks. See Appendices A and B. There was insignificant change between October 2021 and January 2022.”

Rather than eliminating the illegal calls, TCA VOIP amped up the volume. The Complaint indicates (p. 114-116) that on just a single day, Dec. 15, 2021, TCA VOIP relayed more than 10 million calls claiming to be from millions of different USA telephone numbers despite their foreign origin. Barely 0.1% (one tenth of one percent) of the calls lasted more than a minute – a clear indication of automated calling. (By contrast, typical conversational call traffic has more than 40% of the calls lasting more than a minute.)

Anyone with experience looking at robocall traffic knows that the profile described here consists largely of illegal calls. And given the huge daily volume, even if only 5 per cent of the calls were illegal (with the other 95% being, implausibly, legal), that would be half a million illegal calls in a day.

TCA VOIP started getting tracebacks in August of 2020; they met with the Vermont AG and SSA in August of 2021; they kept facilitating calls at a breakneck pace. The FCC issued a Cease-and-Desist³ letter to TCA VOIP on Feb. 10, 2022 – 18 months after that first traceback.

With a timeline like the one in this case (which may or may not be over), it is no wonder that Americans have not seen any significant reduction in illegal robocalls, despite it being a “top priority” at the FCC and within the industry.

³ <https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-tca-voip>

Paragraph 102 of the Complaint says: “TCA VOIP indicated ... that it needed the business from My Country Mobile, TCA VOIP[s]' biggest customer.” TCA VOIP puts these calls on our telephone network because they get paid to do it and it is the core of their business.

The TCA VOIP story is very similar to that of TollFreeDeals / SIP Retail, which was recounted in a Wall Street Journal article⁴ in August of 2020. Dominic Bohnett and Nick Palumbo and John Spiller⁵ and people like them are not going to stop enabling illegal robocallers out of the goodness of their hearts. It is how they make their living.

Stakeholders in the fight against illegal robocalls must sharpen our focus on the small group of individuals and providers that are responsible for the largest fraction of the calls. The Gateway FNPRM attempts to do this with the recognition that many of these calls start in a foreign country. But commenters have expressed myriad misgivings about both the general approach and the details of the FNPRM.

What is so disappointing in the TCA VOIP case is that not only is the massive illegal calling profile apparent in TCA VOIP’s own CDRs, but it would also be apparent to any downstream provider accepting TCA VOIP’s traffic. Each provider doing business with TCA VOIP should have been proactively monitoring that traffic and, given the short-duration profile, demanding justification from TCA VOIP as to its veracity. Given the traffic profile, any provider onboarding TCA VOIP as a new customer should have insisted on knowing exactly what that traffic was before allowing it to surge, in mass volume, onto the network. Those providers taking traffic from TCA VOIP would have seen the tracebacks coming in month after month and THAT certainly should have triggered further scrutiny.

⁴ https://www.wsj.com/articles/where-robocalls-hide-the-house-next-door-11597464021?st=ad2sjx3kz18yjd8&reflink=desktopwebshare_permalink

⁵ Palumbo is the subject of the WSJ article; Spiller is the recipient of the FCC’s largest fine to date: <https://www.fcc.gov/document/fcc-fines-telemarketer-225-million-spoofed-robocalls>

Yet that did not happen, at least to a sufficient degree, because those downstream intermediate providers were happy to get paid to take the calls.

ZipDX estimates that illegal robocallers spend about \$2 million per month on call origination (2 billion calls @ \$0.001 each). By the time that revenue multiplies as it gets paid to the several providers in the call path, it turns into about \$75 million in annual revenue to the telecom industry. If we wiped out illegal robocalling completely, that \$75 million would disappear from the coffers of those providers. This is something that the industry needs to accept, and that Mr. Bohnett admitted to the Vermont AG he was not willing to do. Sure, he's willing to take some steps, but he's not giving up his biggest (and most illegal) customer. We hear similar things from others; yes, they cut off some illegal callers, but not all, and hope that is enough to show their good intentions. Since these providers are so recalcitrant, we have to rely on somebody further downstream to just say no.

USTelecom et al (page 1) say: "Specifically, the Commission should require that all providers implement a robocall mitigation program and provide a certification in the RMD, regardless of that provider's STIR/SHAKEN implementation and its role in transmitting calls. Such approach would ensure the accountability of all providers that touch calls to U.S. consumers, regardless of whether they originate, serve as the gateway provider, or simply transit illegal robocalls."

ZipDX agrees, and we would go a step further to put teeth in that proposal. Any provider that touches an illegal call to a U.S. recipient is finically responsible for the harm done. Such a proviso is necessary to tip the balance away from one that today is purely revenue and profit driven. In this regime, as the Vermont AG and SSA and FCC pursue the next TCA VOIP, the

downstream providers would also be at financial risk for having blindly accepted those millions of calls.

That sounds draconian to some, and vague to others. To make it less vague, we proposed that the FCC be prescriptive, since so many providers seem to need help understanding what it is that they should be doing. Specifically, we said the FCC needs to explain to providers how to distinguish between conversational and non-conversational traffic, and to apply sufficient scrutiny to that non-conversational traffic to ensure its legality – since that is where the robocalls live.

To make it less draconian, we suggested that the FCC offer a safe harbor for conversational traffic. Only those providers that elect to be in the dangerous business of handling non-conversational traffic would incur liability for traffic they had not previously been warned about.⁶

USTelecom says (on page 2): “[T]he Commission should be skeptical of any one-size-fits-all prescriptive requirement. For instance, distinguishing between conversational and short duration non-conversational traffic may be a useful tool for some, including for providers further upstream that accept traffic from lesser known providers. But it may not make sense – or even be viable – where massive amounts of traffic is passed from one provider to another.”

Our structure as a safe harbor means that Verizon, Lumen and AT&T (and any other providers) are free to use whatever approaches they deem best for themselves, given their business circumstances and relationships. They need not avail themselves of this safe harbor if it is not applicable to them. They will assess their financial exposure and act accordingly.

⁶ Contrary to what USTelecom implies, ZipDX has never suggested that non-conversational traffic is always illegal. Rather, we advocate focusing compliance and mitigation efforts on this traffic because that is where the bulk of illegal robocalls are found. USTelecom suggested the possibility of First Amendment issues, but we are not altering the existing rules about what calls are or are not permitted.

The safe harbor gives guidance to those providers that lack the sophistication to conceive and implement their own compliance programs. Critically, it places minimal burden on providers that make their business in conversational traffic. They merely need to monitor average call duration to ensure that each of their customers' traffic meets the conversational metric. Only upon a traceback or other red flag would they need to amp up mitigation efforts.

But those providers that elect to accept *non-conversational* traffic will be incented to reduce their financial risk by implementing compliance measures that ensure that traffic is legal. Intermediate providers will need to engage with their upstreams to vet robocall campaigns, rather than accepting traffic without challenging it. This will push robocall mitigation efforts closer to the source, where it is most effective. It will reduce the incentive to introduce spurious hops into the call path merely to obfuscate the origin of the calls. It will counter the financial pressure for providers to hang onto their worst customers.

USTelecom says (at footnote 4): "Prescriptive traffic analysis rules also may afford bad actors the opportunity to game the system by knowing the criteria they need to avoid." Our approach is explicitly simple specifically to limit the gaming potential.

1. The rules should apply to all calls to U.S. telephone numbers. We do not limit applicability just to calls purporting to come *from* U.S. numbers. Were that limitation in place, the first thing an illegal robocaller would do is start spoofing Canadian numbers, evading the rule and giving the downstream provider an out (and making a mess of legal Canadian calls).
2. We do not distinguish between calls that come from U.S. based providers versus foreigners, because such a distinction has been shown to be problematic. My Country Mobile, for example, currently has three entries in the Robocall Mitigation Database.

Two of the entries have slightly different corporate names but reference the same internet domain; the two Robocall Mitigation Plans are signed by the same individual. One shows an address in the United Arab Emirates, another in Singapore, and the third New York. The Vermont Complaint (p. 104) suggests they are in fact in India. With our approach, we do not need to care.

3. Gaming average call duration is mathematically quite challenging. When you are sending millions of short-duration calls, it is challenging – and expensive – to find enough longer-duration calls to appreciably move that average. That said, the FCC should anticipate updating the safe harbor should behaviors change.

Industry members have expressed concern that providers further down the call path are more distant from the call originator, making it more difficult for them to police their traffic. Our approach encourages them to have more substantive engagements with their upstreams, to ensure those upstreams, and THEIR upstreams, are doing what it takes to vet traffic. And we would think providers would be confident that the FCC would exercise its enforcement discretion to look first to those providers that are in the best position to assess the traffic they are accepting.

We appreciate the opportunity to comment and look forward to the most constructive possible outcome which best furthers our collective objectives.

Respectfully submitted,

DATED: 5 April 2022

/s/ David Frankel
CEO, ZipDX LLC
dfrankel@zipdx.com
Tel: 800-372-6535